30th Conference on Computational Complexity

CCC’15, June 17-19, 2015, Portland, Oregon, USA

Edited by
David Zuckerman
LIPIcs – Leibniz International Proceedings in Informatics

LIPIcs is a series of high-quality conference proceedings across all fields in informatics. LIPIcs volumes are published according to the principle of Open Access, i.e., they are available online and free of charge.

Editorial Board
- Susanne Albers (TU München)
- Chris Hankin (Imperial College London)
- Deepak Kapur (University of New Mexico)
- Michael Mitzenmacher (Harvard University)
- Madhavan Mukund (Chennai Mathematical Institute)
- Catuscia Palamidessi (INRIA)
- Wolfgang Thomas (Chair, RWTH Aachen)
- Pascal Weil (CNRS and University Bordeaux)
- Reinhard Wilhelm (Saarland University)

ISSN 1868-8969

http://www.dagstuhl.de/lipics
## Contents

Preface  
*David Zuckerman* ............................................................... vii

Awards  
................................................................. ix

Conference Organization  
................................................................. xi

External Reviewers  
................................................................. xiii

### Contributed Papers

**Strong Locally Testable Codes with Relaxed Local Decoders**  
*Oded Goldreich, Tom Gur, and Ilan Komargodski*  
........................................ 1

**An Entropy Sunset Inequality and Polynomially Fast Convergence to Shannon Capacity Over All Alphabets**  
*Venkatesan Guruswami and Ameya Velingker*  
........................................ 42

**The List-Decoding Size of Fourier-Sparse Boolean Functions**  
*Ishay Haviv and Oded Regev*  
........................................ 58

**Nonclassical Polynomials as a Barrier to Polynomial Lower Bounds**  
*Abhishek Bhowmick and Shachar Lovett*  
........................................ 72

**Simplified Lower Bounds on the Multiparty Communication Complexity of Disjointness**  
*Anup Rao and Amir Yehudayoff*  
........................................ 88

**How to Compress Asymmetric Communication**  
*Sivaramakrishnan Natarajan Ramamoorthy and Anup Rao*  
........................................ 102

**Majority is Incompressible by \(AC^0[p]\) Circuits**  
*Igor Carboni Oliveira and Rahul Santhanam*  
........................................ 124

**Lower Bounds for Depth Three Arithmetic Circuits with Small Bottom Fanin**  
*Neeraj Kayal and Chandan Saha*  
........................................ 158

**A Depth-Five Lower Bound for Iterated Matrix Multiplication**  
*Suman K. Bera and Amit Chakrabarti*  
........................................ 183

**Factors of Low Individual Degree Polynomials**  
*Rafael Oliveira*  
........................................ 198

**Verifiable Stream Computation and Arthur-Merlin Communication**  
*Amit Chakrabarti, Graham Cormode, Andrew McGregor, Justin Thaler, and Suresh Venkatasubramanian*  
........................................ 217

**Identifying an Honest \(EXP^{NP}\) Oracle Among Many**  
*Shuichi Hirahara*  
........................................ 244
Adaptivity Helps for Testing Juntas
   Rocco A. Servedio, Li-Yang Tan, and John Wright .......................... 264

A Characterization of Hard-to-cover CSPs
   Amey Bhangale, Prahladh Harsha, and Girish Varma .......................... 280

Subexponential Size Hitting Sets for Bounded Depth Multilinear Formulas
   Rafael Oliveira, Amir Shpilka, and Ben Lee Volk ............................... 304

Deterministic Identity Testing for Sum of Read-once Oblivious Arithmetic Branching Programs
   Rohit Gurjar, Arpita Korwar, Nitin Saxena, and Thomas Thierauf .............. 323

Kolmogorov Width of Discrete Linear Spaces: an Approach to Matrix Rigidity
   Alex Samorodnitsky, Ilya Shkredov, and Sergey Yekhanin ......................... 347

On the (Non) NP-Hardness of Computing Circuit Complexity
   Cody D. Murray and R. Ryan Williams .......................................... 365

Circuits with Medium Fan-In
   Pavel Hrubeš and Anup Rao ...................................................... 381

Correlation Bounds Against Monotone NC^1
   Benjamin Rossman ........................................................................ 392

Non-Commutative Formulas and Frege Lower Bounds: a New Characterization of Propositional Proofs
   Fu Li, Iddo Tzameret, and Zhengyu Wang ........................................ 412

The Space Complexity of Cutting Planes Refutations
   Nicola Galesi, Pavel Pudlák, and Neil Thapen .................................... 433

Tight Size-Degree Bounds for Sums-of-Squares Proofs
   Massimo Lauria and Jakob Nordström ............................................. 448

A Generalized Method for Proving Polynomial Calculus Degree Lower Bounds
   Mladen Mikša and Jakob Nordström ................................................ 467

Generalized Quantum Arthur-Merlin Games
   Hirotada Kobayashi, François Le Gall, and Harumichi Nishimura ............... 488

Parallel Repetition for Entangled k-player Games via Fast Quantum Search
   Kai-Min Chung, Xiaodi Wu, and Henry Yuen ....................................... 512

Upper Bounds on Quantum Query Complexity Inspired by the Elitzur-Vaidman Bomb Tester
   Cedric Yen-Yu Lin and Han-Hsuan Lin ............................................. 537

A Polylogarithmic PRG for Degree 2 Threshold Functions in the Gaussian Setting
   Daniel M. Kane ............................................................................. 567

Incompressible Functions, Relative-Error Extractors, and the Power of Nondeterministic Reductions (Extended Abstract)
   Benny Applebaum, Sergei Artemenko, Ronen Shaltiel, and Guang Yang .......... 582

On Randomness Extraction in AC0
   Oded Goldreich, Emanuele Viola, and Avi Wigderson .......................... 601
The papers in this volume were accepted for presentation at the 30th Computational Complexity Conference (CCC’15), held June 17–19, 2015 in Portland, Oregon as part of the ACM Federated Computing Research Conference (FCRC’15). The conference is organized by the Computational Complexity Foundation in cooperation with the European Association for Theoretical Computer Science (EATCS) and the ACM Special Interest Group on Algorithms and Computation Theory (SIGACT). CCC’15 is sponsored by Microsoft Research and is supported by the Institute for Quantum Computing (IQC).

The call for papers sought original research papers in all areas of computational complexity theory. Of the 110 submissions the program committee selected 30 for presentation at the conference.

The program committee would like to thank everyone involved in the conference, including all those who submitted papers for consideration as well as the reviewers (listed separately) for their scientific contributions; the board of trustees of the Computational Complexity Foundation and especially its president Dieter van Melkebeek for extensive advice and assistance; Jacobo Toran for a variety of assistance; Mike Saks for sharing his knowledge as 2014 PC chair; and Marc Herbstritt for coordinating the production of these proceedings.

David Zuckerman
Program Committee Chair
Awards

The program committee of the 30th Computational Complexity Conference is happy to present the 2015 Best Paper Award to Benjamin Rossman for his paper

“Correlation Bounds Against Monotone NC$^1$,”

and the 2015 Best Student Paper Award to Rafael Oliveira for his paper

“Factors of Low Individual Degree Polynomials.”

Funding for the best student paper award is provided by the European Association for Theoretical Computer Science (EATCS).
Conference Organization

Program Committee
Andris Ambainis, University of Latvia
Andrej Bogdanov, Chinese University of Hong Kong
Andrew Drucker, University of Edinburgh
Zeev Dvir, Princeton University
Parikshit Gopalan, Microsoft
Johan Håstad, KTH, Stockholm
Russell Impagliazzo, University of California, San Diego
Prasad Raghavendra, University of California, Berkeley
Ran Raz, Weizmann Institute & IAS
Shubhangi Saraf, Rutgers University
David Zuckerman (chair), University of Texas at Austin

FCRC Liaison
Dieter van Melkebeek, University of Wisconsin-Madison

Board of Trustees
Eric Allender (Treasurer), Rutgers University
Venkatesan Guruswami, Carnegie Mellon University
Jeff Kinne (Secretary), Indiana State University
Dieter van Melkebeek (President), University of Wisconsin-Madison
Madhu Sudan, Microsoft Research New England
Jacobo Toran, University of Ulm
Osamu Watanabe, Tokyo Institute of Technology
External Reviewers

Alex Arkhipov
Salman Beigi
Abhishek Bhowmick
Vladimir Braverman
Christina Brzuska
Siu On Chan
Julia Chuzhoy
Javier Esparza
Yuval Filmus
Nicola Galesi
Alon Gou
Aram Harrow
Christian Ikenmeyer
Michael Kapralov
Subhash Khot
Swastik Kopparty
Chin Ho Lee
Satyanarayana Lokam
Raghu Meka
Dana Moshkovitz
Harikrishna Narayanan
Toni Pitassi
Oded Regev
Rahul Santhanam
Alexander Sherstov
Piyush Srivastava
Ido Tal
Hing Yin Tsang
Dieter van Melkebeek
Marc Vinyals
Carol Wang
Thomas Watson
Karl Wimmer
Ke Yi
Per Austrin
Aleksandrs Belovs
Eric Blais
Jop Briët
Andre Chailloux
Xi Chen
Constantinos Daskalakis
Will Evans
Michael Forbes
Ankit Garg
Joao Gouveia
Prahladh Harsha
Janis Iraids
Tali Kaufman
Hartmut Klauck
Ravi Kumar
Troy Lee
Shachar Lovett
Mladen Miksa
Daniel Nagaj
Jakob Nordström
Sebastian Pokutta
Silas Richelson
Giannicola Scarpa
Seung Woo Shin
David Steurer
Li-Yang Tan
Salil Vadhan
Thomas Vidick
Emanuele Viola
Osamu Watanabe
Omri Weinstein
John Wright
Shengyu Zhang
Raef Bassily
Arnab Bhattacharyya
Fernando Brandao
Joshua Brody
Sourav Chakraborty
Kai-Min Chung
Anindya De
Omar Fawzi
Ariel Gabizon
Sivakant Gopi
Siyao Guo
Sangxia Huang
Erich Kaltofen
Akinori Kawachi
Gillat Kol
Massimo Lauria
Nikos Leonardos
Laura Mancinska
Tomoyuki Morimae
Chandra Nair
Ryan O’Donnell
Igor Razgon
Aviad Rubinstein
Rocco Servedio
Srikanth Srinivasan
Howard Straubing
Luca Trevisan
Greg Valiant
Jevgenijs Vihrovs
Ben Lee Volk
John Watrous
Ryan Williams
Sergey Yekhanin

30th Conference on Computational Complexity (CCC’15).
Editor: David Zuckerman
Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany